METHOD FOR KEY MANAGEMENT OF POINT-TO-POINT COMMUNICATIONS

Patent number: WO9509498
Publication date: 1995-04-06
Inventor: FINKELSTEIN LOUIS DAVID; BROWN DANIEL PETER; PUHL LARRY CHARLES
Applicant: MOTOROLA INC [US]
Classification:
- International: H04L9/00
- european: H04L9/08
Application number: WO1994US09519 19940825
Priority number(s): US19930127718 19930927

Also published as:
EP0671091 (A
US5410602 (A
FI952405 (A)
EP0671091 (A

Cited documents:
US5124117

Abstract of **WO9509498**

A method of secure key distribution in a communication system having a plurality of subscriber units (10 102) and an infrastructure communication center (104) is provided. A first subscriber unit (100) sends a request (202) to the infrastructure communication center (104) for a secure communication link with a second subscriber unit (102). This request includes an encrypted session encryption key which was encrypted with a first subscriber registration key. The infrastructure communication center decrypts the encrypted session encryption key (204) with the first subscriber registration key. Subsequently, the infrastructure communication center re-encrypts the session encryption key (206) with a second subscriber registration key. This re-encrypted session encryption key is sent (210) to the second subscriber unit.

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/00 — A1

(11) International Publication Number: WO 95/09498

(43) International Publication Date: 6 April 1995 (06.04.95)

(21) International Application Number: PCT/US94/09519

(22) International Filing Date: 25 August 1994 (25.08.94)

(30) Priority Data:
08/127,718 27 September 1993 (27.09.93) US

(71) Applicant: MOTOROLA INC. [US/US]; 1303 East Algonquin Road, Schaumburg, IL 60196 (US).

(72) Inventors: FINKELSTEIN, Louis, David; 1698 West Ottowa Court, Wheeling, IL 60090 (US). BROWN, Daniel, Peter; 788 Chatham Avenue, Elmhurst, IL 60126 (US). PUHL, Larry, Charles; 6 Plum Court, Sleepy Hollw, IL 60118 (US).

(74) Agents: PARMELEE, Steven, G. et al.; Motorola Inc., Intellectual Property Dept./ATS, 1303 East Algonquin Road, Schaumburg, IL 60196 (US).

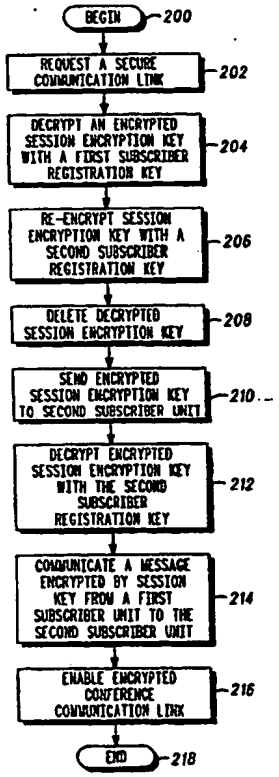
(81) Designated States: FI, JP, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.

(54) Title: METHOD FOR KEY MANAGEMENT OF POINT-TO-POINT COMMUNICATIONS

(57) Abstract

A method of secure key distribution in a communication system having a plurality of subscriber units (100, 102) and an infrastructure communication center (104) is provided. A first subscriber unit (100) sends a request (202) to the infrastructure communication center (104) for a secure communication link with a second subscriber unit (102). This request includes an encrypted session encryption key which was encrypted with a first subscriber registration key. The infrastructure communication center decrypts the encrypted session encryption key (204) with the first subscriber registration key. Subsequently, the infrastructure communication center re-encrypts the session encryption key (206) with a second subscriber registration key. This re-encrypted session encryption key is sent (210) to the second subscriber unit.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	GB	United Kingdom	MR	Mauritania
AU	Australia	GE	Georgia	MW	Malawi
BB	Barbados	GN	Guinea	NE	Niger
BE	Belgium	GR	Greece	NL	Netherlands
BF	Burkina Faso	HU	Hungary	NO	Norway
BG	Bulgaria	IE	Ireland	NZ	New Zealand
BJ	Benin	IT	Italy	PL	Poland
BR	Brazil	JP	Japan	PT	Portugal
BY	Belarus	KE	Kenya	RO	Romania
CA	Canada	KG	Kyrgystan	RU	Russian Federation
CF	Central African Republic	KP	Democratic People's Republic of Korea	SD	Sudan
CG	Congo			SE	Sweden
CH	Switzerland	KR	Republic of Korea	SI	Slovenia
CI	Côte d'Ivoire	KZ	Kazakhstan	SK	Slovakia
CM	Cameroon	LI	Liechtenstein	SN	Senegal
CN	China	LK	Sri Lanka	TD	Chad
CS	Czechoslovakia	LU	Luxembourg	TG	Togo
CZ	Czech Republic	LV	Latvia	TJ	Tajikistan
DE	Germany	MC	Monaco	TT	Trinidad and Tobago
DK	Denmark	MD	Republic of Moldova	UA	Ukraine
ES	Spain	MG	Madagascar	US	United States of America
FI	Finland	ML	Mali	UZ	Uzbekistan
FR	France	MN	Mongolia	VN	Viet Nam
GA	Gabon				

METHOD FOR KEY MANAGEMENT OF POINT-TO-POINT COMMUNICATIONS

Related Inventions

The present invention is related to the following invention which is assigned to the assignee of the present invention. Method and Apparatus for Efficient Real-Time Authentication and Encryption in a Communication System by Brown et al. having U.S. Serial No. 08/084,644, and filed on June 28, 1993.

Field of the Invention

The present invention relates to communication systems and, more particularly, to encryption key management of point-to-point communications.

Background of the Invention

Many communications systems currently use encryption to enhance security of the systems. These communication systems include cellular radio telephone communication system, personal communication systems, paging systems, as well as wireline and wireless data networks. By way of example a cellular communication system will be described below; however, it will be appreciated by those

skilled in the art that the encryption techniques described can be readily extended to other communication systems without departing from the scope and spirit of the present invention. Turning now to cellular communication systems, these systems typically include subscriber units (such as mobile or portable units) which communicate with a fixed network communication unit via radio frequency (RF) communication links. A typical cellular communication system includes at least one base station (i.e., communication unit) and a switching center (i.e., an infrastructure communication center). Present cellular communication systems are designed to encrypt communications on an RF link between a subscriber unit and a base station unit through the use of an encryption key known to both units so that others who intercept the RF link communication link will be unable to listen to the communication (e.g., unable to eavesdrop on a voice conversation).

One such RF link encryption technique is described in the United States Digital Cellular (USDC) standard (known as IS-54 and IS-55) and published by the Electronic Industries Association (EIA), 2001 Eye Street, N.W., Washington, D.C. 20006. The USDC system encryption technique utilizes a series of specialized messages which must be passed between the subscriber unit and a base site communication unit before a session encryption key is known to both units. This encryption key is based upon shared secret data (SSD) in USDC system. For an authentication process an SSD_A key is used. Similarly, for a voice privacy function an SSD_B key is used. For the voice privacy function, the initial transmitted subscriber message contains an authentication response, but no other data is encrypted. The command to begin an encryption process is sent from the service provider (i.e., base site communication unit) to the subscriber after the subscriber has been assigned a traffic channel. Further, current system architecture design is focused on bringing encryption to data as well as voice. Data consists of either synchronous or packet data. Ideally, an encryption key should be provided for each data communication session. In a synchronous data environment, a session key is an encryption key which is used for the duration of a single (e.g., circuit switched) data communication (i.e., "call"). Similarly in a data packet environment, a session key is an encryption key which is used from the time that the communication unit registers with a serving system until the next time that the

communication unit re-registers. In addition, in a previously-cited related invention entitled "Method and Apparatus for Efficient Real-Time Authentication and Encryption in a Communication System" by Brown et al. having U.S. Serial No. 08/084,644, and filed on June 28, 1993, another encryption key is proposed for USDC system which is termed an SSD_C key and which is used for data packet encryption. In these communication systems, packetized data also needs to be encrypted. Packetized data adds an additional problem to the typical encryption process. This is because packets of data may arrive at different times at a subscriber unit of a communication unit (i.e., packet messages are "connectionless"). These packets need to be reassembled and decrypted in the same order in which they were encrypted. In addition, an encryption key can only be negotiated when a subscriber performs a registration. Therefore, a need exists for an encryption technique which can alleviate these problems associated with packetized data.

However, these previously known encryption techniques do not address all of the possible eavesdropping vulnerabilities inherent in a communication channel. Eavesdropping may still occur at other points in the communication channel between the subscriber unit and an endpoint target communication device such as through wiretapping of a land-line phone. Such a communication between a subscriber unit and an endpoint target communication device is termed a "point-to-point" communication. The communication may travel along several different physical communication links before being ultimately coupled via a communication link between the subscriber and target devices. For example in the cellular environment, a user of a subscriber unit may place a voice call to a target communication device located at a place of business. In order for that call to be completed, a communication channel must be set up on an RF link to a base site communication unit. In addition, the communication channel must be extended through the public switched telephone network (PSTN) to the place of business. This place of business may have a private telephone network connected to the PSTN. As a result, the communication channel may also need to be extended through the private network to ultimately connect with the target communication device. Currently, encryption techniques are only being applied to individual components of the entire communication channel (e.g., the RF link in USDC system may be encrypted).

However, this leaves other components such as the PSTN or private network vulnerable to eavesdropping through wiretapping. Therefore, a need also exists for an encryption technique which can alleviate these problems associated with eavesdropping at other points of the communication channel.

Summary of the Invention

These needs and others are substantially met through provision of a method of secure key distribution in a communication system having a plurality of subscriber units and an infrastructure communication center. A first subscriber unit sends a request to the infrastructure communication center for a secure communication link with a second subscriber unit. This request includes an encrypted session encryption key which was encrypted with a first subscriber registration key. The infrastructure communication center decrypts the encrypted session encryption key with the first subscriber registration key. Subsequently, the infrastructure communication center re-encrypts the session encryption key with a second subscriber registration key. This re-encrypted session encryption key is sent to the second subscriber unit. In an alternative method, the first subscriber unit and the infrastructure communication center a priori know a session key. Therefore, the infrastructure communication center only needs to encrypt and send the session encryption key to the second subscriber unit, in response to a request by the first subscriber unit.

Brief Description of the Drawings

FIG. **1** is a block diagram showing a preferred embodiment communication system having a first and a second subscriber unit as well as an infrastructure connecting the subscriber units in accordance with the present invention.

FIG. **2** is a flow chart of a preferred embodiment encryption method used by the first and the second subscriber unit over the infrastructure as shown in FIG. **1** in accordance with the present invention.

FIG. 3 is a flow chart of an alternative preferred embodiment encryption method used by the first and the second subscriber unit over the infrastructure as shown in FIG. 1 in accordance with the present invention.

Detailed Description

FIG. 1 generally depicts a first **100** and a second **102** subscriber communication unit (e.g., a radiotelephone) as well as an infrastructure such as an infrastructure communication center or switch **104** and first **106** and second **108** cellular radio base sites. In the following example the subscriber units **100** and **102** are serviced by the same infrastructure switch **104**. The first subscriber unit **100** forms a communication channel with the first base site **106** by an RF link **110**. Similarly, the second subscriber unit **102** forms a communication channel to the second base site **108** by an RF link **112**. In addition, the first base site **106** and the second base site **108** form communication channels to the infrastructure switch **104** by wirelines **114** and **116**, respectively.

However, it will be appreciated by those skilled in the art that multiple switches (e.g., a cellular switch, a local PSTN switch, and/or a long distance carrier switch) could be used to connect the two subscriber units. In addition, the two subscriber units may be a part of two different cellular systems or one connected to a wireline and one a part of a cellular system. Further, the subscriber units could be communicating data rather than voice over a communication channel such as through an Advanced Radio Data Information Service (i.e., ARDIS® a joint venture between Motorola, Inc, and IBM) or a personal communication system (PCS) which is connected to the PSTN through a Mobile Network Integration (MNI) protocol without departing from the scope and spirit of the present invention.

Referring now to FIG. 2, a flow chart of a preferred embodiment "point-to-point" encryption scheme used by the first **100** and the second **102** subscriber unit over the infrastructure **104**, **106**, and **108** is shown. One of the most important elements of this preferred embodiment encryption scheme is the encryption key management in a "point-to-point" communication system. As is described in USDC

system, each subscriber unit establishes a series of RF link encryption keys (e.g., SSD_A and SSD_B keys) upon registration with a cellular infrastructure network. These encryption keys, which are known to the subscriber unit and the cellular infrastructure network, are also known as registration keys. In addition as proposed by Brown et al., another encryption key, termed an SSD_C key, may be generated by each subscriber unit for use in data encryption. This SSD_C may also generate a session encryption key (SEK) which is valid for use during only one synchronous data communication session or one packet data registration session. The session encryption key (SEK) may be used to encrypt a "point-to-point" communication between the first **100** and the second **102** subscriber units such that the communication may even be encrypted as it passes through the infrastructure switch **104**.

The overall security of a communication channel between the first **100** and the second **102** subscriber units depends upon the secure passing of a session key to both subscriber units. Flowchart elements **200** through **218** outline a preferred embodiment technique for securely passing these session encryption keys. A first subscriber unit **100** makes **202** a request to the infrastructure communication center **104** for a secure communication link with a second subscriber unit **102** via the RF link **110**, first base site **106** and wireline **114**. This request preferably includes a session encryption key (SEK) which has been encrypted with a first subscriber registration key ($SSD1_C$). The infrastructure communication center **104** decrypts **204** the encrypted session encryption key (SEK) with the first subscriber registration key ($SSD1_C$). Subsequently, the infrastructure communication center re-encrypts **206** the session encryption key (SEK) with a second subscriber registration key ($SSD2_C$). At this point the infrastructure communication center **104** no longer needs the decrypted session encryption key and may optionally delete **208** the session key from an infrastructure memory device which temporarily stored the session key. This deleting of the decrypted session key may enhance the overall security of the communication system by eliminating the possibility that someone could get unauthorized access to the session keys by tapping into the infrastructure communication center **104** storage memory. The infrastructure communication center **104** then sends **210** the encrypted session encryption key (SEK) to the second subscriber unit **102** via

wireline **116**, second base site **108** and RF link **112**. The second subscriber unit **102** decrypts **212** the encrypted session encryption key (SEK) with the second subscriber registration key ($SSD2_C$). Finally, a message encrypted by the session encryption key (SEK) is communicated **214** between the first subscriber unit **100** and the second subscriber unit **102** transparently (i.e., without the decryption by the infrastructure) through the infrastructure communication center **104**. This message may be decrypted by either subscriber unit **100** or **102** with the session encryption key (SEK).

This method of session key (SEK) management also works for broadcast messaging systems wherein the encrypted session key (SEK) may be sent in step **210** to a plurality of second subscriber units **102** such that broadcast messages may be encrypted by the session key (SEK).

In addition, an encrypted conference communication link may be enabled **216** by the infrastructure communication center **104** through one of two methods. This type of conference communication link is also known as a fractional-duplex mode of encrypted speech for conference applications. The first subscriber unit **100** would broadcast the session key (SEK) to the other parties in the conference call. Then once the session key (SEK) is established, a conversation can proceed whereby each talker can speak individually to all of the others. A smooth conversation flow requires that either an agreement exist between all participants concerning the order of the talkers (which is common on amateur radio nets), or that an automatic speech detector select the "talker" and route the "talker's" encrypted speech to the other subscriber units. Automatic speech detection and directional routing are common in speakerphone devices for conversations between two endpoints; however, through sophisticated automatic routers at infrastructure communication centers **104** it is possible to handle three or more endpoints at a time. One method for enabling automatic routing by the infrastructure communication center **104** involves decrypting subsequent communications from all of the subscriber units in the conference communication link with the decrypted session encryption key (SEK) which was previously stored in the memory of the infrastructure communication center **104**. Another method for enabling automatic routing by the infrastructure communication center **104**

involves participating subscriber units **100** and **102** providing communication activity information to the infrastructure communication center **104**.

Referring now to FIG. **3**, a flow chart of an alternative preferred embodiment "point-to-point" encryption scheme used by the first **100** and the second **102** subscriber unit over the infrastructure **104**, **106**, and **108** is shown. Flowchart elements **300** through **318** outline the alternative preferred embodiment technique for securely passing these session encryption keys. In this alternative preferred embodiment, the first subscriber unit **100** and the infrastructure communication center **104** a priori know (i.e., have previously determined) the value of the session key (SEK) through the subscriber unit registration process or some other way. Therefore, the first subscriber unit **100** makes **302** a request, without including the session encryption key (SEK), to the infrastructure communication center **104** for a secure communication link with a second subscriber unit **102** via the RF link **110**, first base site **106** and wireline **114**. Subsequently, the infrastructure communication center encrypts **306** the session encryption key (SEK) with a second subscriber registration key ($SSD2_C$). At this point the infrastructure communication center **104** no longer needs the decrypted session encryption key and may optionally delete **308** the session key from an infrastructure memory device which temporarily stored the session key. The infrastructure communication center **104** then sends **310** the encrypted session encryption key (SEK) to the second subscriber unit **102** via wireline **116**, second base site **108** and RF link **112**. The second subscriber unit **102** decrypts **312** the encrypted session encryption key (SEK) with the second subscriber registration key ($SSD2_C$). Finally, a message encrypted by the session encryption key (SEK) is communicated **314** between the first subscriber unit **100** and the second subscriber unit **102** transparently (i.e., without the decryption by the infrastructure) through the infrastructure communication center **104**. This message may be decrypted by either subscriber unit **100** or **102** with the session encryption key (SEK). It will be appreciated by those skilled in the art that an encrypted conference communication link may be enabled **316** for this alternative preferred embodiment encryption scheme in a manner similar to the one

previously described in reference to the preferred embodiment encryption scheme shown in FIG. 2.

Although the invention has been described and illustrated with a certain degree of particularity, it is understood that the present disclosure of embodiments has been made by way of example only and that numerous changes in the arrangement and combination of parts as well as steps may be resorted to by those skilled in the art without departing from the spirit and scope of the invention as claimed. For example, the communication channel could alternatively be an electronic data bus, wireline, optical fiber link, satellite link, or any other type of communication channel.

Claims

What is claimed is:

1. A method of secure key distribution in a communication system having a plurality of subscriber units and an infrastructure communication center, comprising:
   (a) requesting, by a first subscriber unit to the infrastructure communication center, a secure communication link with a second subscriber unit, the request including an encrypted session encryption key, the session encryption key being encrypted with a first subscriber registration key;
   (b) decrypting, by the infrastructure communication center, the encrypted session encryption key with the first subscriber registration key;
   (c) re-encrypting, by the infrastructure communication center, the session encryption key with a second subscriber registration key; and
   (d) sending the encrypted session encryption key to the second subscriber unit.

2. The method of claim 1 further comprising the step of communicating a message encrypted by the session encryption key from the first subscriber unit to the second subscriber unit transparently through the infrastructure communication center.

3. The method of claim 1 further comprising the step of decrypting, by the second subscriber unit, the encrypted session encryption key with the second subscriber registration key.

4. The method of claim 1 wherein the sending step comprises sending the encrypted session encryption key to a plurality of second subscriber units.

5. The method of claim 1 further comprising the step of deleting, by the infrastructure communication center, the decrypted session encryption key from a memory device.

6. The method of claim 1 further comprising the step of enabling an encrypted conference communication link, by the infrastructure communication center, through decrypting subsequent communications from subscriber units with the decrypted session encryption key.

7. The method of claim 1 further comprising the step of enabling an encrypted conference communication link, by participating subscriber units, through providing communication activity information to the infrastructure communication center.

8. The method of claim 1 wherein in the step of requesting, the first subscriber unit and the infrastructure communication center know a priori the session encryption key.

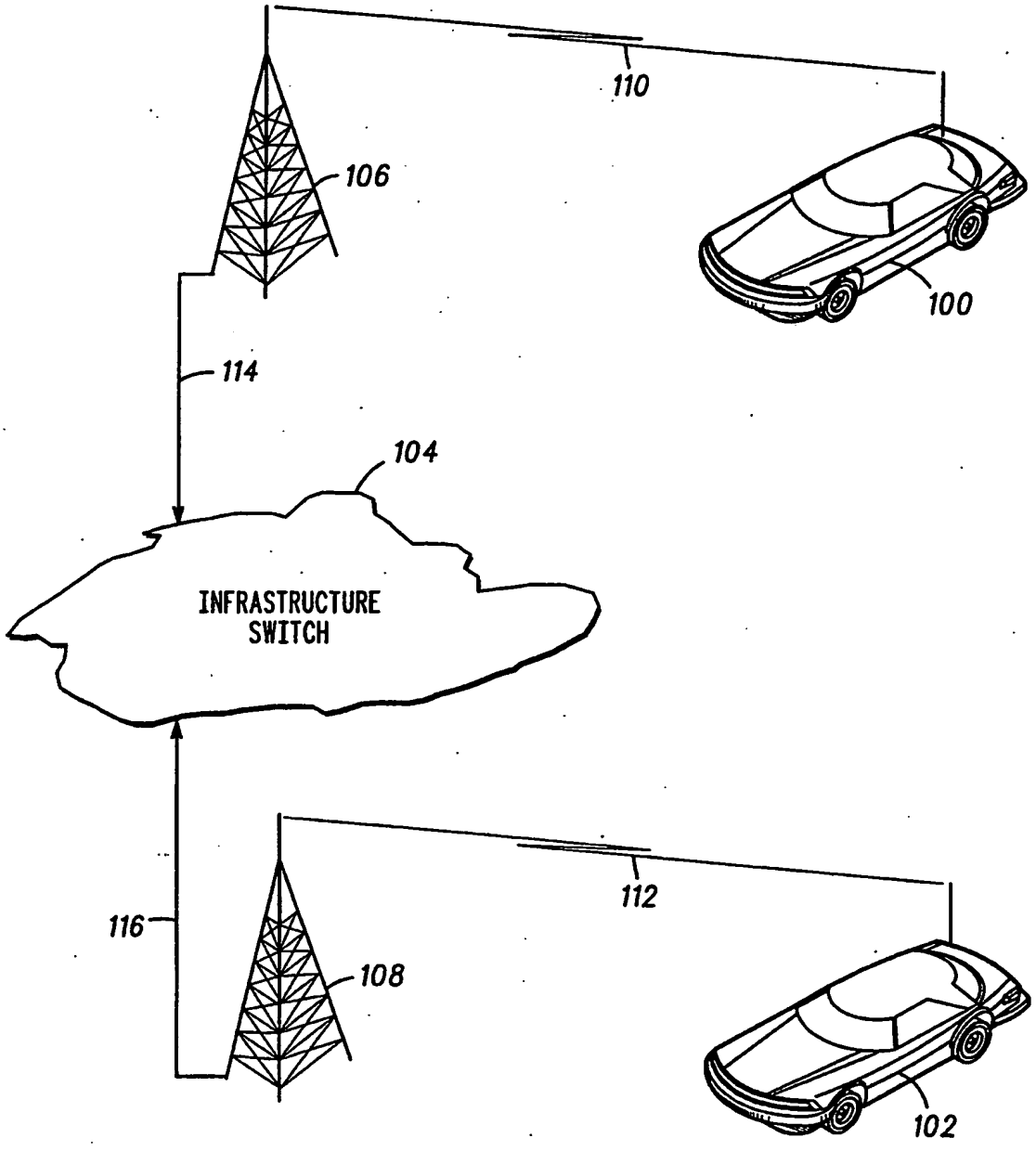


FIG.1

FIG. 2

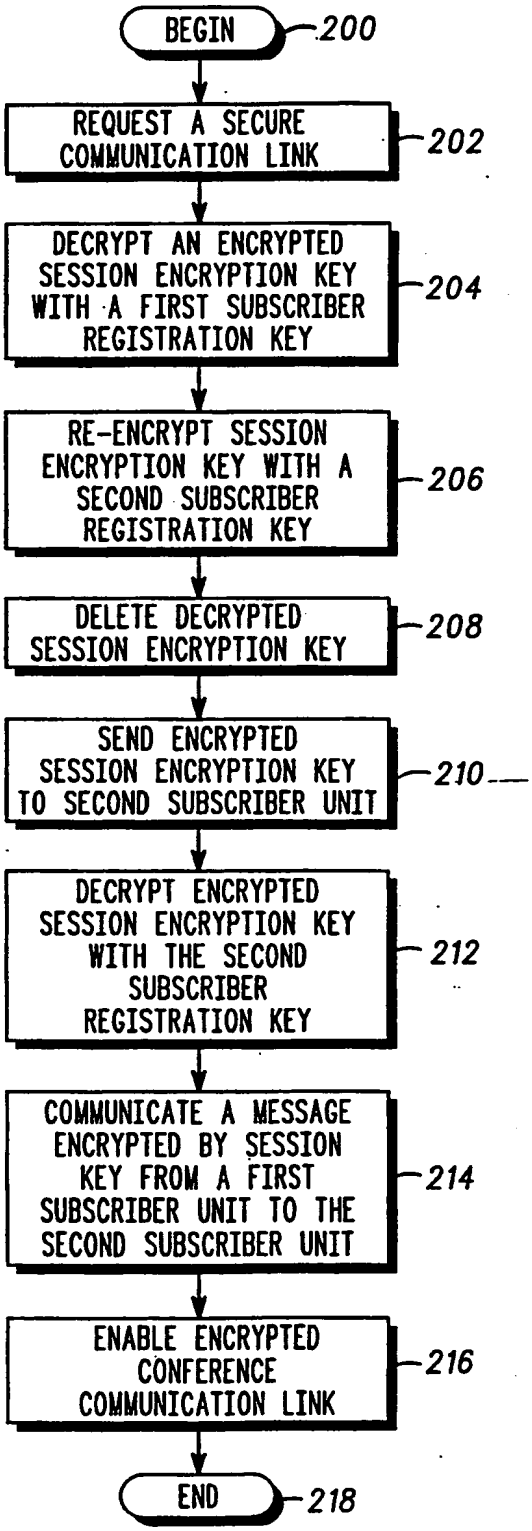
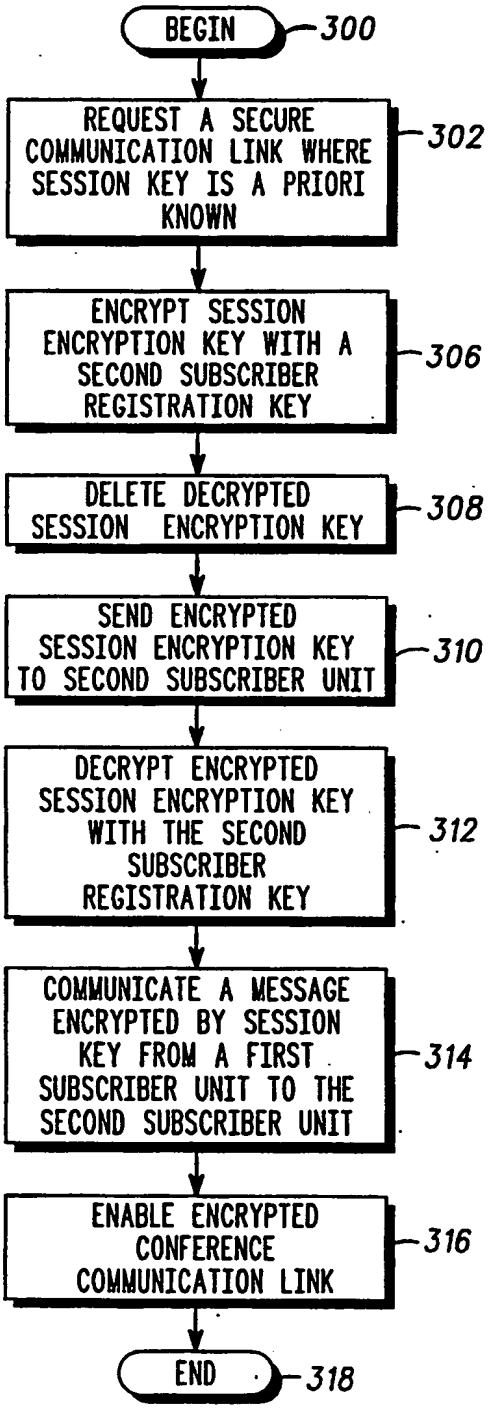

BEGIN
200
REQUEST A SECURE COMMUNICATION LINK
202
DECRYPT AN ENCRYPTED SESSION ENCRYPTION KEY WITH A FIRST SUBSCRIBER REGISTRATION KEY
204
RE-ENCRYPT SESSION ENCRYPTION KEY WITH A SECOND SUBSCRIBER REGISTRATION KEY
206
DELETE DECRYPTED SESSION ENCRYPTION KEY
208
SEND ENCRYPTED SESSION ENCRYPTION KEY TO SECOND SUBSCRIBER UNIT
210
DECRYPT ENCRYPTED SESSION ENCRYPTION KEY WITH THE SECOND SUBSCRIBER REGISTRATION KEY
212
COMMUNICATE A MESSAGE ENCRYPTED BY SESSION KEY FROM A FIRST SUBSCRIBER UNIT TO THE SECOND SUBSCRIBER UNIT
214
ENABLE ENCRYPTED CONFERENCE COMMUNICATION LINK
216
END
218

FIG. 3


BEGIN
300
REQUEST A SECURE COMMUNICATION LINK WHERE SESSION KEY IS A PRIORI KNOWN
302
ENCRYPT SESSION ENCRYPTION KEY WITH A SECOND SUBSCRIBER REGISTRATION KEY
306
DELETE DECRYPTED SESSION ENCRYPTION KEY
308
SEND ENCRYPTED SESSION ENCRYPTION KEY TO SECOND SUBSCRIBER UNIT
310
DECRYPT ENCRYPTED SESSION ENCRYPTION KEY WITH THE SECOND SUBSCRIBER REGISTRATION KEY
312
COMMUNICATE A MESSAGE ENCRYPTED BY SESSION KEY FROM A FIRST SUBSCRIBER UNIT TO THE SECOND SUBSCRIBER UNIT
314
ENABLE ENCRYPTED CONFERENCE COMMUNICATION LINK
316
END
318

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US94/09519

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :H04L 9/00
US CL :380/21, 43
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : Please See Extra Sheet.

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US, A, 5,124,117 (TATEBAYASHI, ET AL.) 23 June 1992	1-8

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be part of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 10 DECEMBER 1994	Date of mailing of the international search report 17 JAN 1995
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer DAVID CAIN Telephone No. (703) 308-0463

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US94/09519

B. FIELDS SEARCHED
Minimum documentation searched
Classification System: U.S.

380/21, 43,30,49